## REMARKS

Applicant has amended claim 15 to correct an inadvertent error and without changing the scope of the claim.

Claims 12-15 are rejected under 35 U.S.C. 103(a). In particular, the Examiner stated:

> Claims 12-15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Roesch et al. (U.S. Patent No. 7,240,368) in view of Shukla (U.S. PG-PUB 2002/0042875).
>
> As per claim 12, Roesch substantially teaches a method for preventing intrusions to a computer system, comprising:
>
> using a network-based appliance to intercept data packets (fig. 2, Router item 20, 6:58-7:10);
>
> deciding whether to forward the intercepted packets or whether to route the intercepted packets to a virtual proxy (6:58-7:10, wherein the IMDS 65 is the virtual proxy);
>
> performing TCP or UDP processing on the intercepted packets before routing them to the virtual proxy (5:43-6:06);
>
> using the virtual proxy to analyze the packets that have been routed to the virtual proxy to detect intrusions using a processing engine having a processing procedure that detects intrusion (i.e., daemon cron 78 detects that intrusions have occurred if new logs are created or logs change sizes, and identifies the source of the packets) (8:01-52).
>
> Kim (sic) fails to teach using the virtual proxy to direct a transport layer to modify packets. However, Shukla discloses modifying packets at the transport layer (paragraphs 0056 and 0087). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to modify the transport layer in order in order to protect the packet from NATs as taught by Shukla (paragraph 0056).
>
> As per claims 13 and 14, Shukla further teaches modifying data in the packets at specified locations and removing data from the packets (paragraphs 0053-0057).
>
> As per claim 15, Kim (sic) further teaches sending a packet stream modification request from an active network-based appliance to a standby network-based appliance to support fault tolerance (7:11-8:23, wherein the).

Applicant has amended claim 15 to correct an inadvertent error and without changing the scope of the claim. As such, Applicant respectfully traverses the Examiner's rejection.

## Discussion of Roesch

Roesch teaches an intrusion deterrence system using a virtual network. As set forth in the Abstract: "The IMDS is a system that creates a synthetic network complete with synthetic hosts and routers. It is comprised of a network server with associated application software that **appears** to be a legitimate portion of a real network to a network intruder. The IMDS consequently invites inquiry and **entices** the intruder away from the real network. … Since there are no legitimate users of the virtual network simulated by the IMDS, **all such activity must be inappropriate and can be**

**treated as such**. Consequently, the entire set of transactions by an intruder can be collected and identified **rather** than just those transactions that meet a predefined attack profile. (Emphasis added)"

Roesch sets forth the following when discussing prior art: (a) at col. 1, lines 36-48: "**Traditional** intrusion detection systems (IDS) protect networks against intruders by **examining the content** of each packet or message passing into the network and **making a determination** as to whether or not it is suspicious, based on pattern matching and a set of general rules. As networks get larger, this approach of looking at every packet presents several drawbacks. One limitation is the speed at which the IDS can process the information ... before it starts to miss packets or degrade system performance."; and (b) at col. 2, lines 21-30: "When packets are routed through router 20 to network 10, they are transmitted to web server 30a, which determines whether the destination is located in network 10. Next, they are transmitted to IDS 30e that then **evaluates the contents, source and destination of each packet to ascertain whether the packet is an intruder**. Once IDS 30e determines the packet is valid, it may then be routed to firewall 30d that again evaluates the source, contents and destination of the packet to ascertain whether the packet may be properly routed to intranet 40. (Emphasis added)"

Roesch sets forth the following in the Summary of the Invention at col. 2, line 60-col. 3, line 11: "Systems and methods consistent with this invention increase the security of computer networks through the use of an Intrusion and Misuse Deterrence System (IMDS) that **passively detects** network intruders in a manner that adds little overhead to a computer network, is adaptive, and easily implemented on any size network. The IMDS creates a synthetic network complete with synthetic hosts and routers. In operation, ... The **IMDS** also **identifies network intruders by monitoring change logs associated with the virtual network, and notifying a system administrator when it notices an adjustment in the size of the change log**. In addition to notifying a system administrator, the IMDS also notifies other network access control devices (e.g., routers, firewalls, etc.) when it detects the presence of an intruder." (Emphasis added)

Roesch states the following at col. 3, line 63-col. 4, line 19: "A system in accordance with the present invention comprises a network server with associated application software that appears to be a legitimate portion of a real network to a network intruder. The **IMDS** consequently invites inquiry and **entices the intruder away from the real network**. ... Valid network users are aware of the

virtual network and its purpose. Consequently, **there are no legitimate users of the virtual network, and all such activity must be inappropriate** and can be treated as such. The ability of the IMDS to detect inappropriate activity based **solely** on the destination of network traffic results in two major benefits. One is that the entire set of transactions by an intruder can be collected and identified rather than just those transactions that meet a predefined attack profile. Second, because the system operates independently of attack type, new exploits and attacks are handled just as effectively as known attacks, resulting in better identification of attack methodologies as well as the identification and analysis of new attack types. ... **Instead of having to watch all of the traffic on a network segment, the IMDS only has to be concerned with the traffic going to its simulated hosts**. (Emphasis added)"

Roesch states the following at col. 6, line 58-col. 7, line 3: "An IMDS access control device in accordance with the subject invention is shown in FIG. 2. IMDS 65 is coupled to network 10 in a manner similar to that of clients 30a e and router 20. It is therefore visible to network users and since it maintains its own collection of seemingly real and vulnerable clients, it is also more attractive to an intruder. **Router 20** is set up such that **any packet 31 with a destination address not in virtual network 60 will be forwarded to firewall 30d**. Any packet with a destination address 44 in virtual network 60 will be forwarded to IMDS 65. The virtual network 60 operating on IMDS 65 is used to attract intruders and log their activity. It is divided into individual virtual or synthetic hosts, each with its own IP address. (Emphasis added)"

Roesch states the following at col. 7, lines 11-59: "IMDS 65 performs three functions: intrusion detection, intrusion notification and system administration. Intrusion detection is accomplished through a set of software packages as shown in FIG. 5, including a network address translator (NAT) 70, a Packet filter 72, an Internet services daemon (inetd) 74, and layered facade services 76. NAT 70 acts as an interface between physical network 10 and virtual network 60. On the physical network 10, NAT 70 connects to a router 20 via link 22. **Router 20, in turn, acts as an interface between IMDS 65 and Internet destinations outside of network 10**. Inside IMDS 65, NAT 70 connects to Packet filter 72 which in turn, is linked to inetd 74 and layered facade services 76. Operation of an intrusion detection function in accordance with the present invention is best explained by way of an example. Assume that an entity operating outside of network 10 sends packet 31 via the Internet to router 20. Packet 31 is destined for IMDS 65 as indicated by IP header

36. That is, destination address 44 equals a destination address in virtual network 60. Upon receiving packet 31, **router 20 routes packet 31 along link 22 to IMDS 65**. ... However, since packet 31 contains a destination address 44 which is not an actual network client, NAT 70 must route the packet to a port 75 in IMDS 65. As shown in FIG. 6, IMDS 65 is also comprised of a plurality of virtual clients 60a c with corresponding IMDS ports 75a i. ... After NAT 70 determines the proper route for packet 31, it sends the packet to Packet filter 72. ... Packet 31 is then passed to inetd 74, which is configured to execute the correct facade service 76 based on the destination port given by NAT 70. The facade service 76 then responds to packet 31 appropriately, and returns the response packet to the original network entity. (Emphasis added)"

Roesch states the following at col. 7, line 63-col. 8, line 23: "Whenever **IMDS 65** determines that an entity has accessed facade services 76, it acts **as if** the entity is an intruder. This is a valid assumption since by definition, all activity on IMDS 65 is of suspect origin. The elements of IMDS 65 that identify an intruder and notify a system administrator are shown in FIG. 7. Specifically, the intruder identification and notification system is comprised of daemon cron 78, notifier routine 80, notification list 82, change logs 84, sendmail routine 86 and at least one administrator mailbox 88. Daemon cron 78 observes applications registered with it and invokes notifier routine 80 when changes are noticed. Notification list 82 contains a list of all network locations. Change logs 84 store data records for each network access event. That is, **each time an entity attempts to access an IMDS port 75, change log 84 creates and stores a data record identifying the transaction**. The recorded changes comprise packets of processed information that typically are used by system administrators for creating audit trails, failure recovery, and undo operations. Since they identify the source of the packet, these records may also be used to identify a network intruder. Sendmail routine 86 composes email messages and routes the messages to mailboxes 88 using information received from notifier routine 80. In operation, the intruder identification and notification process associated with IMDS 65 executes commands found in "crontab" files located in daemon cron 78. These commands specify the operations to be performed and the network entities to be notified when an intruder is detected. (Emphasis added)"

Lastly, Roesch states the following at col. 8, lines 24-30: "As shown in FIG. 8, the operation of the intruder identification and notification system begins in step 810 with daemon cron 78 monitoring a predefined collection of virtual network clients 60. **It does this by keeping track of**

**what change logs 84 exist and their size. If any new logs 84 are created (step 820) or any logs change size (step 830), daemon cron 78 invokes notifier routine 80 in step 840**. (Emphasis added)"

In light of the above, Applicant respectfully submits that Roesch teaches a method and system wherein **IMDS 65**, even if it is considered to be a virtual proxy, does **not analyze packets** to detect intrusions. Instead, Roesch "detects" intrusions by "keeping track of change logs and their size. As set forth in Roesch, "If any new logs 84 are created (step 820) or any logs change size (step 830), daemon cron 78 invokes notifier routine 80." The reason for this, as set forth above, is that Roesch **assumes** that any packet destined for IMDS 65 corresponds to an intrusion.

As to claim 12: The Examiner asserts that "using the virtual proxy to analyze the packets that have been routed to the virtual proxy to detect intrusions using a processing engine having a processing procedure that detects intrusion (i.e., daemon cron 78 detects that intrusions have occurred if new logs are created or logs change sizes, and identifies the source of the packets) (8:01-52)."

Applicant respectfully submits that the Examiner is incorrect. In particular, as discussed above, daemon cron 78 is a routine that detects the occurrence of an intrusion, but it does **not analyze** the packet to detect the intrusion. In fact, it is the Examiner that points out "daemon cron 78 detects that intrusions have occurred if new logs are created or logs change sizes, and identifies the source of the packets." Thus, Applicant respectfully submits that checking to determine whether new logs are created or logs change sizes **is not** analyzing packets. Although, daemon cron 78 identifies the source of packets, it only does this for sending an e-mail and **not** to detect intrusions.

The Examiner further asserts that: Roesch "fails to teach using the virtual proxy to direct a transport layer to modify packets. However, Shukla discloses modifying packets at the transport layer (paragraphs 0056 and 0087). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to modify the transport layer in order in order to protect the packet from NATs as taught by Shukla (paragraph 0056)."

Applicant respectfully submits that the Examiner is incorrect for several reasons. **First**, at paragraph 0056, Shukla teaches **encapsulating** "the transport layer data and header with another transport layer header to protect it from NAT. Shukla goes on to teach that in doing this only the outer transport layer header will get modified while the internal transport layer data and packet **will**

**be left intact**. **Second**, Applicant respectfully submits that the motivation of combining Roesch and Shukla asserted by the Examiner has no relevance to the analysis of obviousness because the motivation to "protect the packet from NATs" has nothing whatsoever to do with solving the problem faced by the inventor because the problem solved by the invention of claim 12 is a method of preventing intrusions. **Third**, even assuming a person of ordinary skill in the art were to combine Roesch and Shukla in the manner asserted by the Examiner (he/she would not), Applicant respectfully submits that that person would not arrive at the invention of claim 12 because of the elements missing from Roesch and from Shukla (as set forth above).

As such, Applicant respectfully submits that claim 12 is patentable over Roesch in view of Shukla.

As to claim 13: Claim 13 depends from Claim 12. As such, Applicant respectfully submits that Claim 13 is patentable over Roesch in view of Shukla for the same reasons set forth above with respect to claim 12. In addition, there is nothing in Roesch or in Shukla that teaches or suggests, in any manner whatsoever, the step of using the virtual proxy to direct the transport layer to modify data in the packets at specified locations. As the Examiner can readily appreciate, Roesch merely provides notification of received packets by IDMS 65 and in no way teaches that the packets are modified after they are received by IDMS 65. Further Shukla does not teach removing data from packets, Shukla merely teaches methods for providing end-to-end secure communications that are compatible with network protocols such as NAT. As such, no person of ordinary skill in the art would combine Roesch and Shukla as asserted by the Examiner because Roesch does not teach that the packets will be transmitted to the so-called "real" network after IDMS 65 is "finished" with them.

As such, Applicant respectfully submits that claim 13 is patentable over Roesch in view of Shukla.

As to claim 14: Claim 14 depends from Claim 12. As such, Applicant respectfully submits that Claim 14 is patentable over Roesch in view of Shukla for the same reasons set forth above with respect to claim 12. In addition, Applicant respectfully submits that the additional arguments set forth above with respect to claim 13 apply here as well.

As such, Applicant respectfully submits that claim 14 is patentable over Roesch in view of Shukla.

As to claim 15: Claim 15 depends from Claim 12. As such, Applicant respectfully submits that Claim 15 is patentable over Roesch in view of Shukla for the same reasons set forth above with respect to claim 12. In addition, the Examiner asserts that "IDMS is the standby appliance since, if an attack is detected, the IDMS is affected, but the rest of the active network, remains in tact." Applicant respectfully submits that the Examiner is incorrect since the Examiner asserts that IDMS 65 is the "virtual proxy" **and** the standby network-based appliance at the same time. This is clearly incorrect for several reasons. **First**, as pointed out, even if one assumes that IDMS 65 of Roesch is a virtual proxy (it is not), IDMS 65 of Roesch does not direct the transport layer to modify packets using packet stream modification requests. **Second**, even if one assumes that IDMS 65 directs the transport layer to modify packets using packet stream modification requests (it does not), there is no teaching hint or suggestion of any kind to send the packet stream modification requests to a standby network based appliance.

As such, Applicant respectfully submits that claim 15 is patentable over Roesch in view of Shukla.

In light of the above, Applicants respectfully request that the Examiner withdraw this rejection.

Accordingly, Applicants submit that the present Application is in condition for allowance. Applicants therefore request reconsideration of the outstanding rejections and issue a Notice of Allowance. The Examiner is invited to contact the undersigned at 650-427-1052 to discuss any additional changes the Examiner may feel is necessary in light of this Amendment.

Date: April 13, 2009

Respectfully submitted,

/Michael B. Einschlag/

3401 Hillview Avenue
Palo Alto, California 94304
Phone: (650) 427-1052

Michael B. Einschlag
Reg. No. 29,301
Attorney for the Applicant